CLAIMS

What is claimed is:

1. A method comprising:

   associating a first entity with a second entity in a first device; and

   selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device.

2. The method as recited in Claim 1, wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

3. The method as recited in Claim 1, wherein the first entity includes a first user, the second entity includes a second user, and wherein without requiring the second entity to be operatively associated with either the first or second device includes without requiring the second user to be logged in to either the first or second device.

4. The method as recited in Claim 1, wherein selectively providing information about the association of the first and second entity to the second device further includes providing the second device with a validation code that identifies the first entity and the second entity, when the first entity is operatively associated with the second device.

5. The method as recited in Claim 4, wherein the validation code identifies the second entity by an identifier and a name.

6. The method as recited in Claim 5, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

7. The method as recited in Claim 4, wherein providing the second device with the validation code further includes encrypting at least a portion of the validation code.

8. The method as recited in Claim 1, wherein associating the first entity with the second entity in the first device further includes logically associating a first entity profile with a second entity profile.

9. The method as recited in Claim 3, wherein the first entity is a parent/guardian of the second entity.

10. The method as recited in Claim 1, wherein the first device includes a network server that is configured to act as an authentication server.

11. The method as recited in Claim 10, wherein the second device includes a network server that is configured to act as an affiliated server associated with the authentication server.

12. A computer-readable medium having computer-executable instructions, comprising:

associating a first entity with a second entity in a first device; and

causing the first device to selectively provided information about the association of the first and second entities to a second device when directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device.

13. The computer-readable medium as recited in Claim 12, wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

14. The computer-readable medium as recited in Claim 12, wherein the first entity includes a first user, the second entity includes a second user, and wherein without requiring the second entity to be operatively associated with either the first or second device includes without requiring the second user to be logged in to either the first or second device.

15. The computer-readable medium as recited in Claim 12, wherein causing the first device to selectively provide information about the association of the first and second entities to the second device further includes providing the second device with a validation code that identifies the first entity and the second entity, when the first entity is operatively associated with the second device.

16. The computer-readable medium as recited in Claim 15, wherein the validation code identifies the second entity by an identifier and a name.

17. The computer-readable medium as recited in Claim 16, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

18. The computer-readable medium as recited in Claim 15, wherein causing the first device to provide the second device with the validation code further includes encrypting at least a portion of the validation code.

19. The computer-readable medium as recited in Claim 12, wherein associating the first entity with the second entity in the first device further includes logically associating a first entity profile with a second entity profile.

20. The computer-readable medium as recited in Claim 14, wherein the first user is a parent/guardian of the second user.

21. The computer-readable medium as recited in Claim 12, wherein the first device includes a network server that is configured to act as an authentication server.

22. The computer-readable medium as recited in Claim 21, wherein the second device includes a network server that is configured to act as an affiliated server associated with the authentication server.

23. An apparatus comprising:

memory having information associating a first user of the apparatus with a second user of the apparatus; and

logic operatively coupled to the memory and configured to respond to inputs from the first user by selectively outputting the information about the association of the first user and the second user, without requiring the second user to be operatively signed-in to the apparatus.

24. The apparatus as recited in Claim 23, wherein the logic is configurable to be operatively connected to at least one external device and is further configured to selectively output the information within a validation code that identifies the first user and the second user, when the first user signs-in to the external device.

25. The apparatus as recited in Claim 24, wherein the validation code identifies the second user by an identifier and a name.

26. The apparatus as recited in Claim 24, wherein the validation code identifies modifications to a consent parameter associated with the second user.

27. The apparatus as recited in Claim 24, wherein the logic is further configured to encrypt at least a portion of the validation code.

28. The apparatus as recited in Claim 23, wherein the logic is further configured logically associate a first user profile with a second user profile in the memory.

29. The apparatus as recited in Claim 23, wherein the first user is a parent/guardian of the second user.

30. The apparatus as recited in Claim 23, wherein the apparatus is included in a network server that is configured to act as an authentication server.

31. The apparatus as recited in Claim 30, wherein the external device includes a network server that is configured to act as an affiliated server associated with the authentication server.

32. A computer-readable medium having stored thereon a data structure, comprising:

a validation code that identifies a first entity and a second entity.

33. The computer-readable medium as recited in Claim 32, wherein the first entity and the second entity are selected from a group of entities

that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

34. The computer-readable medium as recited in Claim 32, wherein the validation code identifies the second entity by an identifier and a name.

35. The computer-readable medium as recited in Claim 33, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

36. The computer-readable medium as recited in Claim 34, wherein at least a portion of the validation code is encrypted.

37. An apparatus comprising:

memory; and

logic operatively coupled to the memory and configured to allow a first entity to be operatively associated with the apparatus, and receive information about an association of the first entity and at least one other entity, without requiring the at least one other entity to be operatively associated with the apparatus.

38. The apparatus as recited in Claim 36, wherein the first entity and the at least one other entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

39. The apparatus as recited in Claim 36, wherein the first entity includes a first user, the at least one other entity includes a second user, and wherein without requiring the at least one other entity to be operatively associated with the apparatus includes without requiring the second user to be logged in to the apparatus.

40. The apparatus as recited in Claim 36, wherein the logic is configurable to receive the information about the association from an external device via a validation code that identifies the first entity and the at least one other entity, when the first entity is operatively associated with the external device.

41. The apparatus as recited in Claim 39, wherein the validation code identifies the at least one other entity by an identifier and a name.

42. The apparatus as recited in Claim 39, wherein the validation code identifies modifications to a consent parameter associated with the at least one other entity.

43. The apparatus as recited in Claim 39, wherein the logic is further configured to decrypt the validation code, as needed.

44. The apparatus as recited in Claim 39, wherein, in response to the validation code, the logic is further configurable to output previously

gathered information relating to the at least one other entity to the external device.

45. The apparatus as recited in Claim 38, wherein the first user is a parent/guardian of the second user.

46. The apparatus as recited in Claim 36, wherein the apparatus is included in a network server that is configured to act as an affiliate server.

47. The apparatus as recited in Claim 39, wherein the external device includes a network server that is configured to act as an authentication server.